

**RECEIVED  
CENTRAL FAX CENTER****OCT 12 2005**

Intellectual Property Department  
170 Wood Avenue South  
Iselin, New Jersey 08830  
Tel: 732-321-3023  
Fax: 732-321-3030  
Email: Alexander.burke@siemens.com

**SIEMENS****Fax**

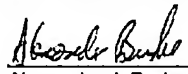
<b>To:</b>	Examiner: Zachary A. Davis	<b>From:</b>	Alexander J. Burke
<b>Fax:</b>	571-273-8300	<b>Pages:</b>	37
<b>Phone:</b>	571-272-3870	<b>Date:</b>	October 12, 2005
<b>Re:</b>	Application of: Barry Lynn Royer et al. Serial No. 09/817,320 Art Unit: 2137		

IF YOU DO NOT RECEIVE ALL OF THIS TELEFAX IN GOOD ORDER,

PLEASE CALL: Christine Briscoe at 732-321-3018Attached is the following: Appeal Brief 36 ppAppeal Brief 33 pp

For Application No.: 09/817,320  
Filing Date: March 26, 2001  
First Named Inventor: Barry Lynn Royer et al.  
Group Art Unit: 2137  
Attorney Docket: 2001P04781US

**RECEIVED  
OIPE/IAP****OCT 13 2005**

<b>CERTIFICATE OF TRANSMISSION UNDER 37 CFR 1.8</b>	
I hereby certify that this correspondence is being facsimile transmitted to the U.S. Patent and Trademark Office	
	<u>12 October 2005</u>
Alexander J. Burke Reg. No. 40,425	Date

Serial No.: 09/817,320

01P04781US

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED  
CENTRAL FAX CENTERBefore the Board of Patent Appeals and Interferences

OCT 12 2005

Applicant : Barry Lynn Royer et al.

Serial No. : 09/817,320

Filed : March 26, 2001

For : A SYSTEM AND USER INTERFACE SUPPORTING URL  
PROCESSING AND CONCURRENT APPLICATION OPERATION

Examiner : Zachary A. Davis

Art Unit : 2137

APPEAL BRIEF

May It Please The Honorable Board:

Appellants appeal the Final Rejection, dated May 13, 2005, of Claims 1 - 22 of the above-identified application. The fee of five hundred dollars (\$500.00) for filing this Brief and any associated extension fee is to be charged to Deposit Account No. 19-2179. Enclosed is a single copy of this Brief.

Please charge any additional fee or credit any overpayment to the above-identified Deposit Account.

Appellants do not request an oral hearing.

10/14/2005 BABRAHA1 00000040 192179 09817320

01 FC:1402 500.00 DA

Serial No.: 09/817,320

01P04781US01

**I. REAL PARTY IN INTEREST**

The real party in interest of Application Serial No. 09/817,320 is the Assignee of record:

Siemens Medical Solutions Health Services Corporation  
51 Valley Stream Parkway  
Malvern, PA 19355-1406

**II. RELATED APPEALS AND INTERFERENCES**

There are currently, and have been, no related Appeals or Interferences regarding Application Serial No. 09/817,320.

**III. STATUS OF THE CLAIMS**

Claims 1 - 11 and 13 - 22 are rejected and the rejection of claims 1 - 11 and 13 - 22 are appealed. Claim 12 was not specifically rejected, but it was objected to. However, it was also argued and appealed here.

**IV. STATUS OF AMENDMENTS**

All amendments were entered and are reflected in the claims included in Appendix I.

**V. SUMMARY OF CLAIMED SUBJECT MATTER**

Independent claim 1 recites a system employed by an application for encoding URL link data for use in detecting unauthorized URL modification. A link processor for processing URL data by identifying an address portion of the URL, encrypting the address portion of the URL, incorporating the encrypted address portion of the URL, together with the address portion of the URL in non-encrypted form, into a single processed URL data string (page 1, line 37 - page 2, line 3) and providing a key supporting decryption of the

Serial No.: 09/817,320

01P04781US01

encrypted address portion to a destination system (page 13, line 35-page 14, line 3). A communication processor for incorporating the processed URL data string into formatted data for communication to the destination system (page 2, lines 3-5).

Dependent claim 2 includes the features of independent claim 1 along with the additional feature that the link processor adaptively identifies the address portion as URL data either (a) lying between "http://" and a question mark "?" or (b) lying between "http://" and a pound/number sign "#," in response to whichever of condition (a) and (b) is satisfied first (page 9, lines 36-page 10, line 1).

Dependent claim 3 includes the features of independent claim 1 and the additional feature that the link processor adaptively identifies the address portion based on the application associated with the URL (page 10, lines 21-36).

Dependent claim 4 includes the features of independent claim 1 and dependent claim 3, along with the additional feature that the link processor adaptively uses (a) an address portion for ASP (Active Server Page) applications comprising a SERVER\_NAME and SCRIPT\_NAME and (b) an address portion for a non-ASP applications comprising a SERVER\_NAME, SCRIPT\_NAME and PATH\_INFO (page 10, lines 28-33).

Dependent claim 5 includes the features of independent claim 1 along with the additional feature that the processor compresses the address portion of the URL prior to encryption and incorporation into the processed URL data string (page 11, lines 26-28).

Serial No.: 09/817,320

01P04781US01

Dependent claim 6 includes the features of independent claim 1 and dependent claim 5, along with the additional feature that the link processor converts the address portion of the URL to lower case before compression (page 10, lines 3-4).

Dependent claim 8 includes the features of independent claim 1 along with the additional feature that the link processor incorporates at least one of, (a) a session identifier, identifying a particular session of user initiated operation of the application and (b) an encrypted patient identifier, into the processed URL data string (page 11, lines 1-9).

Dependent claim 9 includes the features of independent claim 1 and dependent claim 8, along with the additional feature that the link processor incorporates the session identifier into the processed URL data string by formatting the session identifier into a data field including the session identifier and encrypted address separated by a colon (that is, session identifier:encrypted address) (page 11, lines 9-20; page 13, lines 7-11).

Dependent claim 10 includes the features of independent claim 1, along with the additional feature that the link processor concatenates the address portion of the URL together with data associated with a personal record to form a data element, and encrypts the data element for incorporation into the single processed URL data string (page 12, lines 6 – 27).

Dependent claim 12 includes the features of independent claim 1, along with the additional feature that the link processor encodes the address portion of the URL using an RSA (Rivest Shamir Adleman) MD5 compatible hashing function (page 10, lines 6-10).

Serial No.: 09/817,320

01P04781US01

Independent claim 13 recites a system employed by an application for encoding URL link data for use in detecting unauthorized URL modification. A link processor processes URL data by identifying an address portion of the URL, encrypting the address portion of the URL, incorporating the encrypted address portion of the URL, together with the address portion of the URL in non-encrypted form (page 1, line 37 – page 2, line 3) and a session identifier identifying a user session of computer operation, into a single processed URL data string (page 11, lines 1-2). A communication processor incorporates the processed URL data string into formatted data for communication to a request device (page 2, lines 3-5).

Dependent claim 14 includes the features of independent claim 13, along with the additional feature that the link processor compresses the identified address portion and encrypts the compressed address portion of the URL to provide the encrypted address portion (page 11, lines 26-28). The link processor converts the identified address portion to lower case prior to compressing the identified address portion using a hash function (page 10, lines 3-4).

Independent claim 15 recites a system employed by an application for decoding URL link data encoded for use in detecting unauthorized URL modification. An input processor for receiving an encoded URL (page 2, lines 8-12). A link processor for processing the encoded URL by identifying an encrypted address portion of the received encoded URL and a corresponding non-encrypted address portion of the received encoded URL (page 13, lines 20-25), decrypting the encrypted address portion of the URL to provide a decrypted URL address portion (page 13, lines 12-13; 32-37). A validation processor for determining if the decrypted URL address portion has been subject to unauthorized modification by determining if the decrypted URL address portion is

Serial No.: 09/817,320

01P04781US01

different to the corresponding non-encrypted address portion of the received encoded URL (page 13, lines 15 – 19).

Dependent claim 16 includes the features of independent claim 15, along with the additional feature that the decrypted URL address portion is a first hash value (page 13, lines 32-33). The validation processor applies a hashing function to the corresponding non-encrypted address portion of the received encoded URL to provide a comparison second hash value (page 13, lines 22 – 25) and compares the comparison second hash value with the first hash value, and upon a match determines a successful validation of the received encoded URL (page 13, lines 12 – 19; page 14, lines 4 – 6).

Independent claim 20 recites a method employed by an application for encoding URL link data for use in detecting unauthorized URL modification. An address portion of a URL is identified. The address portion of the URL is encrypted. The encrypted address portion of the URL, together with the address portion of the URL in non-encrypted form, is incorporated into a single processed URL data string (page 1, line 37 – page 2, line 3). A key supporting decryption of the encrypted address portion to a destination system is provided (page 13, line 35 page 14, lines 2-3). The processed URL data string is incorporated into formatted data for communication to the destination system (page 2, lines 3-5).

Independent claim 21 recites a method employed by an application for decoding URL link data encoded for use in detecting unauthorized URL modification. An encoded URL is received (page 2, lines 6-12). An encrypted address portion of the received encoded URL and a corresponding non-encrypted address portion of the received encoded URL are identified (page 2, lines 6-12 and page 13, lines 22-25). The encrypted address

Serial No.: 09/817,320

01P04781US01

portion of the received encoded URL is decrypted to provide a decrypted URL address portion (page 13, lines 12-13). It is determined if the decrypted URL address portion has been subject to unauthorized modification by determining if the decrypted URL address portion is different to the corresponding non-encrypted address portion of the received encoded URL (page 13, lines 15-19).

#### VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-3, 5, 7-13 and 15-22 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent 5,708,780 – Levergood.

Claims 4, 6 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood (U.S. Patent 5,708,780).

#### VII. ARGUMENT

Levergood neither anticipate nor make unpatentable the present claimed invention. Thus, reversal of the Final Rejection (hereinafter termed “rejection”) of claims 1–22 under 35 U.S.C. §§ 102(b) and 103(a) is respectfully requested.

#### Overview of the Cited References

Levergood describes a method for controlling and monitoring access to network servers. The process includes client-server sessions over the Internet involving hypertext files. When the user selects a link on a hypertext document or page that is directed to an access-controlled file, the server subjects the request to a secondary server which determines whether the client has an authorization or valid account. Upon such verification, the user is



Serial No.: 09/817,320

01P04781US01

provided with a session identification which allows the user to access the requested file as well as any other files within the present protection domain.

**Rejection of Claims 1-3, 5, 7-13 and 15-22 under 35 U.S.C. 102(b)**  
**over Levergood (U.S. Patent 5,708,780)**

Reversal of the Final Rejection (hereinafter termed "rejection) of claims 1-3, 5, 7-13 and 15-22 under 35 U.S.C. 102(b) as being anticipated by US Patent 5,708,780 issued to Levergood is respectfully requested because the rejection makes crucial errors in interpreting the cited reference. The rejection erroneously states that claims 1-3, 5, 7 - 13 and 15-22 are anticipated by Levergood.

**CLAIMS 1, 5, 7, 8 and 11**

Claim 1 recites a system "employed by an application for encoding URL link data for use in detecting unauthorized URL modification" comprising "a link processor for processing URL data by identifying an address portion of said URL, encrypting said address portion of said URL, incorporating said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string and providing a key supporting decryption of said encrypted address portion to a destination system; and a communication processor for incorporating said processed URL data string into formatted data for communication to said destination system." These features are not shown (or suggested) in Levergood.

Serial No.: 09/817,320

01P04781US01

The system of claim 1 involves “encrypting said address portion of said URL, incorporating, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string.” As well as “providing a key supporting decryption of said encrypted address portion, to a destination system,” for use in decrypting the “encrypted address portion” by the “destination system.” These features address the security deficiencies of URL processing functions of electronic systems. “Applications are vulnerable to the corruption of URL data and the context information conveyed within the URL data. The URL data conveyed from application 200 to application 230 includes context information comprising a session identifier and optionally a user or patient identifier. This URL data is potentially vulnerable to corruption to cause URL replay or redirection of an application to a substitute address or to gain access to application functions and parameters for unauthorized purposes. In order to protect against such corruption and to ensure that the entity being accessed is the one originally targeted, portions of the URL data conveyed between applications are advantageously encrypted” (Application page 10, line 37 – page 11, line 9).

The claimed system addresses the security problem by ensuring “that a URL link (e.g. a URL link to child application 230) embedded in a web page provided for display using browser 10 is not redirected. For this purpose, application 200 generates a hash value from the domain, path, program, and program data portion of the URL. Application 200 (as the sending application) generates a hash value from the fully qualified URL link” (Application page 9 lines 32-37). “Application 230 decrypts the received hash value for comparison with a corresponding hash value independently generated from corresponding URL data retrieved from a web server.” Specifically, the “independently generated hash value and the hash value received by application 230 from application 200 via browser 10

Serial No.: 09/817,320

01P04781US01

are compared and if they are not equal, the request to initiate application 230 is rejected” (Application page 10 lines 25-37).

Levergood does not show or suggest “**encrypting said address portion of said URL** incorporating, said encrypted address portion of said URL, together with said address portion of said URL in **non-encrypted form**, into a single processed URL data string” for decryption by a “destination system” using the provided “key supporting decryption of said encrypted address portion.” Levergood does not show or suggest “providing a key supporting decryption of said encrypted address portion, to a destination system,” for use in decrypting the “encrypted address portion” by the “destination system” as in the present claimed invention. In an exemplary embodiment of the invention illustrated in the Application specification pages 11-13, application 200 advantageously, for example, encrypts “a **URL link address portion**” comprising a hash value identified by field identifier GSH= derived by “hashing on the **addressable portion** of a fully qualified URL” comprising the “URL data either lying between the “http://” and the question mark “?” or from the data lying between the “http://” and the pound/number sign “#” - whichever comes first” (Application page 10 lines 1-2 and page 11 line 25-27). Consequently, in the exemplary URL string shown processed in the specification page 12:

www.smed.com/altoona/prd/results.exe/1?GSM=16253384937&GSH=24017&Pid  
=1772693&Frclt=blue

the compressed address portion is 24017 which is concatenated with a patient identifier (Application page 12 line lines 17-21) as shown:

GSH=24017&Pid=1772693

Serial No.: 09/817,320

01P04781US01

and is encrypted into the string

16sfdjwhejeyw7rh3hekw

to produce the processed URL including the encrypted URL address portion:

www.smed.com/altoona/prd/results.exe/1?GSM=16253384937:16sfdjwhejeyw7rh3  
hekw&Frgclr=blue.

This is an exemplary “processed URL.” The Rejection makes a **fundamental error** on page 4 in interpreting the Levergood reference. Contrary to the Rejection statements on page 4, Levergood in column 5 lines 61-65 and column 3 lines 34-37 relied on in the Rejection merely discloses encryption of a session identifier (SID) and an IP address. Specifically, Levergood states “the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers” (Levergood, column 5 lines 61-65, also see column 3 lines 33-37).

Further, although in Levergood a valid session identifier “typically comprises” an “accessible domain” in the “SID encrypted with a secret key,” the Levergood accessible domain is NOT a URL or an address portion of a URL (Levergood et al., column 3 lines 33-37). Levergood explicitly defines an accessible “domain” as a collection of files and NOT a URL or address portion of a URL (“A protection domain is defined by the service provider and is a collection of controlled files of common protection within one or more servers” – Levergood, column 3 lines 52-55). This is further made clear in column 5 lines

Serial No.: 09/817,320

01P04781US01

54-61 stating a "preferred SID is a sixteen character ASCII string that encodes 96 bits of SID data" that contains "an 8-bit domain comprising a set of information files to which the current SID authorizes access." Such an "accessible domain" as used by Levergood is not in a URL link address portion. This is further corroborated in column 6 lines 29-34 of Levergood indicating that a domain is in the non-address, URL data field portion of a URL (e.g. after the question mark), specifically, a "REDIRECT URL might be: "http://auth.com/authenticate?domain= [domain]& URL = http://content.com/report."

In the Advisory Action it is asserted that if the domain includes a collection of files within a server, then the "domain must include an identification and/or address for these files," thus the domain can indeed include an address portion of a URL. However, nowhere in Levergood is it disclosed or suggested that the domain includes a URL or even a portion of a URL. In fact, Levergood explicitly defines a protection domain as "a collection of controlled files of common protection within one or more servers" in column 3, lines 52-55. The Advisory Action interpreting "a collection of files" to anticipate "encrypting said address portion of said URL" makes a fundamental error in interpreting the Levergood reference. In so doing, the Advisory Action engages in the pure speculation that the Levergood "collection of files" has something to do with a URL, but also that it leads to teaching encryption of an "address portion of said URL" as specifically defined in the present Application. Further, this speculation is without foundation and directly contradicts Levergood's own teaching in column 5 line 59 that a domain is an 8-bit value ("SID data" contains "an 8-bit domain comprising a set of information files"). Thus, Levergood neither discloses nor suggests "a link processor for processing URL data" as in the present claimed invention.

Levergood does not show or suggest "encrypting said address portion of said

Serial No.: 09/817,320

01P04781US01

URL.” Neither a session identifier nor an IP address as used in Levergood is a “URL or a URL address portion.” Indeed a URL and IP address are distinct and different objects with totally different functions (“the content server records the URL and the IP address” – Levergood column 5, lines 37-38). An IP address describes an electronic address of an Internet entity whereas a URL “consists of three parts: the transfer format, the host name of the machine that holds the file, and the path to the file” (Levergood column 2, lines 28-31). A session identifier identifies a user session of computer operation for example and is itself a distinct entity that may be conveyed within a field of a URL (Application page 11, line 22).

Levergood also does not show or suggest the claim 1 feature combination involving “incorporating, said encrypted address portion of said URL, together with said address portion of said URL in **non-encrypted form**, into a single processed URL data string” for decryption by a “destination system” using the provided “key supporting decryption of said encrypted address portion.” Contrary to the Rejection statement on page 4 and as explained previously, the SID of Levergood does NOT contain an “encrypted address portion” of a URL. Further, the purpose of the Levergood encryption is to ensure validity of session identifiers (SIDs) by using an “Internet server” to subject “the client to an authorization routine prior to issuing the SID” (Levergood column 3 lines 24-26). In contrast, the Application addresses the problem of preventing “URL replay or redirection” through its recognition that URLs are “vulnerable to corruption” (Application page 11, lines 1-9). Consequently, there is no reason, problem recognition or motivation for amending the Levergood system to include the claimed arrangement. Consequently, withdrawal of the rejection of claim 1 under 35 USC 102(b) is respectfully requested.

Serial No.: 09/817,320

01P04781US01

Dependent claims 5, 7, 8 and 11 are considered to be patentable for the reasons given in connection with claim 1. Consequently, as the Levergood system neither discloses nor suggests each element of the claimed arrangement, Levergood does not anticipate the invention claimed in claims 5, 7, 8 and 11. Therefore, withdrawal of the rejection of claims 5, 7, 8 and 11 under 35 USC 102(b) is respectfully requested.

### CLAIM 2

Dependent claim 2 is considered to be patentable based on its dependence on claim 1. Therefore, the arguments presented above with respect to claim 1 also apply to claim 2. Claim 2 is also considered to be patentable because Levergood neither discloses nor suggests a "link processor" that "adaptively identifies said address portion as URL data either, (a) lying between "http://" and a question mark "?" or (b) lying between "http://" and a pound/number sign "#", in response to whichever of condition (a) and (b) is satisfied first." Contrary to the Rejection statement on page 4 and as explained in connection with claim 1, Levergood in column 3, line 56 to column 4, line 18 does not provide any description of adaptively identifying an "address portion" of a URL based on "whichever" of a "condition (a) and (b) is satisfied first." Specifically, adaptively identifying an "address portion" as "URL data either, (a) lying between "http://" and a question mark "?" or (b) lying between "http://" and a pound/number sign "#", in response to whichever of condition (a) and (b) is satisfied first." Levergood also shows no recognition of the problem this feature addresses.

In view of the above remarks regarding claim 2, it is respectfully submitted that the present invention as claimed in claim 2 is not anticipated by Levergood.

Serial No.: 09/817,320

01P04781US01

CLAIM 3

Dependent claim 3 is considered to be patentable based on its dependence on claim 1. Therefore, the arguments presented above with respect to claim 1 also apply to claim 3. Claim 3 is also considered to be patentable because Levergood does not show (or suggest) "adaptively" identifying the "address portion based on the application associated with said URL." Contrary to the Rejection statement on page 4, Levergood, in column 3, line 56 to column 4, line 18, does not provide any 35 USC 112 compliant enabling description of such a feature.

In view of the above remarks regarding claim 3, it is respectfully submitted that the present invention as claimed in claim 3 is not anticipated by Levergood.

CLAIM 9

Dependent claim 9 is considered to be patentable based on its dependence on claim 1. Therefore, the arguments presented above with respect to claim 1 also apply to claim 9. Claim 9 is also considered to be patentable because Levergood does not show (or suggest) a "link processor" that "incorporates said session identifier into said processed URL data string by formatting said session identifier into a data field including said session identifier and encrypted address separated by a colon (that is, session identifier:encrypted address)." Levergood does NOT show or suggest such features in the cited column 3, lines 12-16 or elsewhere.

In view of the above remarks regarding claim 9, it is respectfully submitted that the present invention as claimed in claim 9 is not anticipated by Levergood.



Serial No.: 09/817,320

01P04781US01

CLAIM 10

Dependent claim 10 is considered to be patentable based on its dependence on claim 1. Therefore the arguments presented above with respect to claim 1 also apply to claim 10. Claim 10 is also considered to be patentable because Levergood does not show (or suggest) a "link processor" that "concatenates said address portion of said URL together with **data associated with a personal record** to form a data element, and encrypts said data element for incorporation into said single processed URL data string." The Levergood system in cited column 3, lines 34-37 or elsewhere does not show selection of a URL address portion at all and does not show or suggest a "link processor" that "concatenates said address portion of said URL together with **data associated with a personal record** to form a data element" as claimed in claim 10. Levergood also does not show or suggest encryption of "said data element for incorporation into said single processed URL data string."

In view of the above remarks regarding claim 10, it is respectfully submitted that the present invention as claimed in claim 10 is not anticipated by Levergood.

CLAIM 12

As the status of the rejection of claim 12 is unclear from the Office Action, Applicant has addressed claim 12 with respect to the rejection of the claims under 35 U.S.C. 102(b) as being anticipated by US Patent 5,708,780 issued to Levergood. Dependent claim 12 is considered to be patentable based on its dependence on claim 1. Therefore the arguments presented above with respect to claim 1 also apply to claim 12. Claim 12 is also considered to be patentable because Levergood neither discloses nor

Serial No.: 09/817,320

01P04781US01

suggests the "link processor encodes said address portion of said URL using an RSA (Rivest Shamir Adleman) MD5 compatible hashing function."

The arguments concerning the patentability of claim 12 are provided in the event the Office Action intended to include a rejection of this claim. Only an objection to claim 12 was explicitly indicated in both the Office Action and the Advisory Action.

In view of the above remarks regarding claim 12, it is respectfully submitted that the present invention as claimed in claim 12 is not anticipated by Levergood.

### CLAIM 13

Independent claim 13 includes similar limitations and is considered to be patentable for the reasons given in connection with claims 1 and 8. Claim 13 is also considered to be patentable because Levergood in column 3, lines 12-16, 34-37, column 5, lines 52-65, column 4 and column 7 or elsewhere do not show (or suggest) a feature combination including "a link processor for processing URL data" by "encrypting said address portion of said URL, incorporating, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form and a session identifier identifying a user session of computer operation, into a single processed URL data string." Levergood does not show (or suggest) such features for the reasons given in connection with the previous claims.

In view of the above remark and the remarks concerning claims 1 and 8, it is respectfully submitted that claim 13 of the present invention is not anticipated by Levergood.

Serial No.: 09/817,320

01P04781US01

CLAIMS 15, 17-19

Independent claim 15 includes similar limitations and is considered to be patentable for the reasons given in connection with claim 1. Claim 15 is also considered to be patentable because Levergood does not show or suggest "an encrypted address portion of said received encoded URL and a corresponding non-encrypted address portion of said received encoded URL" as claimed in claim 15 of the present invention. Neither a session identifier nor an IP address as used in Levergood, is a "URL or URL address portion." As discussed hereinabove with specific reference to claim 1, a URL and IP address are distinct and different objects with totally different functions ("the content server records the URL and the IP address" – Levergood column 5, lines 37-38). An IP address describes an electronic address of an Internet entity whereas a URL "consists of three parts: the transfer format, the host name of the machine that holds the file, and the path to the file" (Levergood column 2, lines 28-31). A session identifier identifies a user session of computer operation for example and is itself a distinct entity that may be conveyed within a field of a URL (Application page 11, line 22). Thus, neither a session IP nor an IP address is equivalent to "an encrypted address portion of said received encoded URL" as in the present claimed invention.

Further, Levergood does not show (or suggest) a feature combination that detects "unauthorized URL modification" by "decrypting said encrypted address portion of said URL to provide a decrypted URL address portion" and "determining if said decrypted URL address portion has been subject to unauthorized modification by determining if said decrypted URL address portion is different to said corresponding non-encrypted address portion of said received encoded URL." The Levergood digital signature comparison relied on in column 6, lines 5-16 is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID"

Serial No.: 09/817,320

01P04781US01

(Levergood column 3, lines 24-26). In contrast, the Application addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11, lines 1-9). Consequently, there is no reason, problem recognition or motivation for amending the Levergood system to include the claimed arrangement. Consequently, Levergood does not show or suggest "decrypting said encrypted address portion of said URL to provide a decrypted URL address portion." Further, Levergood does not show or suggest (and are incapable of) "determining if said decrypted URL address portion has been subject to unauthorized modification by determining if said decrypted URL address portion is different to said corresponding non-encrypted address portion of said received encoded URL."

In view of the above remarks, it is respectfully submitted that claim 15 of the present invention is not anticipated by Levergood for the reasons discussed above. Claims 17-19 are also considered patentable due to their dependence on claim 15. Consequently, as the Levergood system neither discloses nor suggests each element of the claimed arrangement, Levergood does not anticipate the invention claimed in claims 15 and 17-19. Therefore, withdrawal of the rejection of claims 15 and 17-19 under 35 USC 102(b) is respectfully requested.

#### CLAIM 16

Dependent claim 16 is considered to be patentable based on its dependence on claim 15. Therefore the arguments presented above with respect to claim 15 also apply to claim 16. Claim 16 is also considered to be patentable because, contrary to the assertions in the Office Action, Levergood in column 6, lines 5-16 does not show (or suggest) a system in which "said decrypted URL address portion is a first hash value, and said validation processor, applies a hashing function to said corresponding non-encrypted

Serial No.: 09/817,320

01P04781US01

address portion of said received encoded URL to provide a comparison second hash value, and compares said comparison second hash value with said first hash value, and upon a match determines a successful validation of said received encoded URL" indicating no "unauthorized URL modification." Levergood does not suggest such a feature combination or contemplate comparing hash values representing URL address portions. Additionally, Levergood does not contemplate or provide a system for determining "unauthorized URL modification."

In view of the above remarks, it is respectfully submitted that claim 16 of the present invention is not anticipated by Levergood for the reasons discussed above.

#### CLAIM 20

Independent claim 20 is a method claim mirroring apparatus claim 1 and is considered to be patentable for the reasons given in connection with claim 1.

In view of the above remarks, it is respectfully submitted that claim 20 of the present invention is not anticipated by Levergood for the reasons discussed above. Therefore, withdrawal of the rejection of claim 20 under 35 USC 102(b) is respectfully requested.

#### CLAIM 21 and 22

Independent claim 21 is a method claim mirroring apparatus claim 15 and is considered to be patentable for the reasons given in connection with claim 15.

Serial No.: 09/817,320

01P04781US01

In view of the above remarks, it is respectfully submitted that claim 21 of the present invention is not anticipated by Levergood for the reasons discussed above. Claim 22 is dependent on claim 21 and thus is also considered to be patentable for the reasons given in connection with claim 21. Consequently, as the Levergood system neither discloses nor suggests each element of the claimed arrangement, Levergood does not anticipate the invention claimed in claims 21 and 22. Therefore, withdrawal of the rejection of claims 21 and 22 under 35 USC 102(b) is respectfully requested.

In view of the above remarks, Applicant respectfully submits that there is no 35 USC 112 compliant enabling disclosure present in Levergood that anticipates the present invention as claimed in independent claims 1, 13, 15, 20 and 21. As claims 2-3, 5 and 7-12 are dependent on claim 1, claims 16-19 are dependent on claim 13, and claim 22 is dependent on claim 21, Applicant respectfully submits that claims 2-3, 5, 7-12, 16-19 and 22 are also not anticipated by Levergood. It is thus respectfully submitted that this rejection is satisfied and should be withdrawn.

**Rejection of Claims 4, 6 and 14 under 35 USC 103(a) over Levergood et al.**

**(U.S. 5,708,780)**

Claims 4, 6 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,708,780 – Levergood. These claims are deemed to be patentable for the reasons given below.

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the examiner to establish a factual basis to support the legal conclusion of obviousness. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596, 1598 (Fed.Cir. 1988). In so doing, the Examiner is expected to

Serial No.: 09/817,320

01P04781US01

make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (CCPA 1966), and to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention. Such reason must stem from some teaching, suggestion, or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the art. *Uniroya, Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed.Cir. 1988), *cert. denied*, 488 U.S. 825 (1988); *Ashland Oil Inc. v. Delta Resins & Refractories, Inc.*, 776 F.2d 28, 293, 227 USPQ 657, 664 (Fed.Cir. 1985), *cert. denied*, 475 U.S. 1017 (1986); *ACS Hosp. Sys., Inc. v. Montefiore Hosp.*, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed.Cir. 1984). These showings by the Examiner are an essential part of complying with the burden of presenting a *prima facie* case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed.Cir. 1992).

#### CLAIM 4

Dependent claim 4 is considered to be patentable based on its dependence on claims 1 and 3. Claim 4 is also considered to be patentable because Levergood does not show (or suggest) a "link processor" that "adaptively uses (a) an address portion for ASP (Active Server Page) applications comprising a SERVER\_NAME and SCRIPT\_NAME and (b) an address portion for a non-ASP applications comprising a SERVER\_NAME, SCRIPT\_NAME, and PATH\_INFO." As recognized in the Rejection on page 7, Levergood et al. do not disclose the use of Active Server Page applications. However, the Rejection takes Official Notice that "use of Active Server Page applications" is well known and would have been obvious to use in the claim 4 arrangement (Rejection page 7 lines 7-11). It is acceptable for official notice to be taken of a fact of "wide notoriety", *In re Howard*, 394 F. 2d 869, 157 USPQ 615, 616 (CCPA 1968) e.g. a fact commonly known to laymen everywhere, 29 AM. Jur 2D Evidence S. 33 (1994) or of a fact that is

Serial No.: 09/817,320

01P04781US01

capable of "instant and unquestionable demonstration", In re Ahlert 424 F. 2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970). However, official notice should not be taken of a fact normally subject to the possibility of rational disagreement among reasonable men, In re Eynde, 480 F. 2d 1364, 1370; 178 USPQ 470, 474 (CCPA 1973). It is submitted that the elements of which the Rejection takes official notice, in the context of their respective claims, are neither features of "wide notoriety", (In re Howard), nor capable of "instant and unquestionable demonstration" (In re Ahlert). On the contrary, these features are subject to the possibility of rational disagreement given the claim arrangements within which they reside. Consequently, Applicants take exception to this instance of official notice used in the Rejection. Further, the Applicant requests that a showing be made of evidence that these features were well known, in the context of their respective claims at the time the invention was made. It is submitted that on the contrary, Levergood fails to recognize any need for adaptive URL generation responsive to whether an Active Server Page is involved or not. Levergood does not mention use of Active Server Pages at all. Consequently, withdrawal of the rejection of claim 4 under 35 USC 103(a) is respectfully requested.

#### CLAIM 6

Dependent claim 6 is considered to be patentable based on its dependence on claim 1. Claim 6 is also considered to be patentable because Levergood does not show (or suggest) a "link processor" that "converts said address portion of said URL to lower case before compression." Contrary to the Rejection statement on page 7, Levergood does not provide any 35 USC 112 compliant enabling description of such a feature. Levergood fails to recognize any need for case sensitive conversion. Levergood does not mention lower case or upper case at all. Consequently, withdrawal of the rejection of claim 6 under 35 USC 103(a) is respectfully requested.



Serial No.: 09/817,320

01P04781US01

CLAIM 14

Dependent claim 14 is considered to be patentable based on its dependence on claim 13. Claim 14 is also considered to be patentable because Levergood does not show (or suggest) a "link processor" that "compresses said identified address portion and encrypts said compressed address portion of said URL to provide said encrypted address portion and said link processor converts said identified address portion to lower case prior to compressing said identified address portion using a hash function." However, the Rejection takes Official Notice that "URLs are case sensitive," that a "hash function" is sensitive to uppercase and lower case characters and that as a result "forcing all characters" to lower case in the context of the claimed arrangement of claim 14 would have been obvious (Rejection page 8 lines 1-6). It is acceptable for official notice to be taken of a fact of "wide notoriety", In re Howard, 394 F. 2d 869, 157 USPQ 615, 616 (CCPA 1968) e.g. a fact commonly known to laymen everywhere, 29 AM. Jur 2D Evidence S. 33 (1994) or of a fact that is capable of "instant and unquestionable demonstration", In re Ahlert 424 F. 2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970). However, official notice should not be taken of a fact normally subject to the possibility of rational disagreement among reasonable men, In re Eynde, 480 F. 2d 1364, 1370; 178 USPQ 470, 474 (CCPA 1973). It is submitted that the elements of which the Rejection takes official notice, in the context of their respective claims, are neither features of "wide notoriety," (In re Howard), nor capable of "instant and unquestionable demonstration" (In re Ahlert). On the contrary, these features are subject to the possibility of rational disagreement given the claim arrangements within which they reside. Especially, given that alternative options exist such as the use of a non-case sensitive compression algorithm, for example. Consequently, Applicants take exception to this instance of official notice used in the Rejection. Further, Applicants request that a showing be made of evidence that these features were well

Serial No.: 09/817,320

01P04781US01

known, in the context of their respective claims at the time the invention was made. It is submitted that on the contrary, Levergood fails to show or suggest a "link processor" that "compresses said identified address portion and encrypts said compressed address portion of said URL to provide said encrypted address portion and said link processor converts said identified address portion to lower case prior to compressing said identified address portion using a hash function." Levergood also does not suggest such a feature combination for reasons given in connection with claims 1 and 6. Consequently, withdrawal of the rejection of claim 14 under 35 USC 103(a) is respectfully requested.

In view of the above remarks, Applicants submit that the Application is in condition for allowance, and favorable reconsideration is requested.

### VIII CONCLUSION

Neither Levergood nor the Official Notice alone or in combination with one another discloses a system employed by an application for encoding URL link data for use in detecting unauthorized URL modification. Levergood and the Official Notice neither disclose nor suggest "a link processor for processing URL data" as in the present claimed invention. Additionally Levergood and the Official Notice neither disclose nor suggest "identifying an address portion of said URL" as in the present claimed invention. Also, Levergood and the Official Notice neither disclose nor suggest "encrypting said address portion of said URL" as in the present claimed invention. Additionally Levergood and the Official Notice neither disclose nor suggest "incorporating said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string" as in the present claimed invention. Levergood and the Official Notice also neither disclose nor suggest "providing a key supporting decryption of

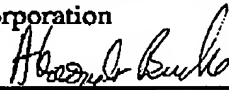
Serial No.: 09/817.320

01P04781US01

said encrypted address portion, to a destination system" as in the present claimed invention. Furthermore, Levergood and the Official Notice neither disclose nor suggest "a communication processor for incorporating said processed URL data string into formatted data for communication to said destination system" as in the present claimed invention.

Accordingly it is respectfully submitted that the rejection of Claims 1- 22 should be reversed.

Respectfully submitted,  
Siemens Medical Solutions Health Services  
Corporation



Alexander J. Burke  
Reg. No. 40,425

Date: October 12, 2005

Alexander J. Burke  
Customer No. 28524  
Tel. 732 321 3023  
Fax 732 321 3030

Serial No.: 09/817,320

01P04781US01

**APPENDIX I - APPEALED CLAIMS**

1. (Previously Presented) A system employed by an application for encoding URL link data for use in detecting unauthorized URL modification, comprising:

a link processor for processing URL data by

identifying an address portion of said URL,

encrypting said address portion of said URL,

incorporating said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string and

providing a key supporting decryption of said encrypted address portion, to a destination system; and

a communication processor for incorporating said processed URL data string into formatted data for communication to said destination system.

2. (Previously presented) A system according to claim 1, wherein said link processor adaptively identifies said address portion as URL data either,

(a) lying between "http://" and a question mark "?" or

(b) lying between "http://" and a pound/number sign "#", in response to whichever of condition (a) and (b) is satisfied first.

3. (Original) A system according to claim 1, wherein said link processor adaptively identifies said address portion based on the application associated with said URL.

Serial No.: 09/817,320

01P04781US01

4. (Original) A system according to claim 3, wherein said link processor adaptively uses (a) an address portion for ASP (Active Server Page) applications comprising a SERVER\_NAME and SCRIPT\_NAME and (b) an address portion for a non-ASP applications comprising a SERVER\_NAME, SCRIPT\_NAME, and PATH\_INFO.

5. (Original) A system according to claim 1, wherein said link processor compresses said address portion of said URL prior to encryption and incorporation into said processed URL data string.

6. (Original) A system according to claim 5, wherein said link processor converts said address portion of said URL to lower case before compression.

7. (Original) A system according to claim 5, wherein said link processor compresses said address portion using at least one function from (a) a hash function, (b) another compression function.

8. (Previously presented) A system according to claim 1, wherein said link processor incorporates at least one of, (a) a session identifier, identifying a particular session of user initiated operation of said application and (b) an encrypted patient identifier, into said processed URL data string.

9. (Original) A system according to claim 8, wherein said link processor incorporates said session identifier into said processed URL data string by formatting said session identifier into a data field including said session identifier and encrypted address separated by a colon (that is, session identifier:encrypted address).

Serial No.: 09/817,320

01P04781US01

10. (Original) A system according to claim 1, wherein said link processor concatenates said address portion of said URL together with data associated with a personal record to form a data element, and encrypts said data element for incorporation into said single processed URL data string.

11. (Original) A system according to claim 10, wherein said data associated with a personal record is at least one of, (a) a patient identifier, (b) a user identifier, (c) an encounter identifier and (d) an observation identifier.

12. (Previously Presented) A system according to claim 1, wherein said link processor encodes said address portion of said URL using an RSA (Rivest Shamir Adleman) MD5 compatible hashing function.

13. (Previously Presented) A system employed by an application for encoding URL link data for use in detecting unauthorized URL modification, comprising:

- a link processor for processing URL data by
  - identifying an address portion of said URL,
  - encrypting said address portion of said URL,
  - incorporating said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form and a session identifier identifying a user session of computer operation, into a single processed URL data string;
- and
- a communication processor for incorporating said processed URL data string into formatted data for communication to a request device.

Serial No.: 09/817,320

01P04781US01

14. (Previously presented) A system according to claim 13, wherein  
said link processor compresses said identified address portion and encrypts  
said compressed address portion of said URL to provide said encrypted address portion and  
said link processor converts said identified address portion to lower case  
prior to compressing said identified address portion using a hash function.

15. (Previously presented) A system employed by an application for  
decoding URL link data encoded for use in detecting unauthorized URL modification,  
comprising:

an input processor for receiving an encoded URL;  
a link processor for processing said encoded URL by  
identifying an encrypted address portion of said received encoded  
URL and a corresponding non-encrypted address portion of said received encoded URL,  
decrypting said encrypted address portion of said URL to provide a  
decrypted URL address portion,  
a validation processor for determining if said decrypted URL address  
portion has been subject to unauthorized modification by determining if said decrypted  
URL address portion is different to said corresponding non-encrypted address portion of  
said received encoded URL.

16. (Previously presented) A system according to claim 15, wherein said  
decrypted URL address portion is a first hash value, and  
said validation processor,

Serial No.: 09/817,320

01P04781US01

applies a hashing function to said corresponding non-encrypted address portion of said received encoded URL to provide a comparison second hash value, and

compares said comparison second hash value with said first hash value, and upon a match determines a successful validation of said received encoded URL.

17. (Original) A system according to claim 15, wherein said link processor identifies and extracts a session identifier from a non-encrypted portion of said received encoded URL.

18. (Original) A system according to claim 15, wherein said decrypted URL address portion includes data associated with a personal record.

19. (Original) A system according to claim 18, wherein said data associated with a personal record is at least one of, (a) a patient identifier and (b) a user identifier.

20. (Previously presented) A method employed by an application for encoding URL link data for use in detecting unauthorized URL modification, comprising the steps of:

identifying an address portion of a URL;

encrypting said address portion of said URL;

incorporating, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string;



Serial No.: 09/817,320

01P04781US01

providing a key supporting decryption of said encrypted address portion to a destination system; and

incorporating said processed URL data string into formatted data for communication to said destination system.

21. (Previously presented) A method employed by an application for decoding URL link data encoded for use in detecting unauthorized URL modification, comprising the steps of:

receiving an encoded URL;

identifying an encrypted address portion of said received encoded URL and a corresponding non-encrypted address portion of said received encoded URL;

decrypting said encrypted address portion of said received encoded URL to provide a decrypted URL address portion; and

determining if said decrypted URL address portion has been subject to unauthorized modification by determining if said decrypted URL address portion is different to said corresponding non-encrypted address portion of said received encoded URL.

22. (Previously presented) A method according to claim 21, wherein said decrypted URL address portion is a first hash value, and including the steps of

applying a hashing function to said corresponding non-encrypted address portion of said received encoded URL to provide a comparison second hash value, and

comparing said comparison second hash value with said first hash value, and upon a match determining a successful validation of said received encoded URL.

Serial No.: 09/R17,320

01P04781US01

**APPENDIX II - EVIDENCE**

Applicant does not rely on any additional evidence other than the arguments submitted hereinabove.

Serial No.: 09/817,320

01P04781US01

**APPENDIX III - RELATED PROCEEDINGS**

Applicant respectfully submits that there are no proceedings related to this appeal in which any decisions were rendered.

Serial No.: 09/817,320

01P04781US01

**APPENDIX IV - TABLE OF CASES**

1. *In re Howard*, 394 F. 2d 869, 157 USPQ 615, 616 (CCPA 1968)
2. 29 AM. Jur 2D Evidence S. 33 (1994)
3. *In re Ahlert*, 424 F. 2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970)
4. *In re Eynde*, 480 F. 2d 1364, 1370; 178 USPQ 470, 474 (CCPA 1973)

**APPENDIX V - LIST OF REFERENCES**

<b><u>U.S. Pat. No.</u></b>	<b><u>Issued Date</u></b>	<b><u>102(e) Date</u></b>	<b><u>Inventors</u></b>
5,708,780	January 13, 1998		Levergood et al.

Serial No.: 09/817,320

01P04781US01

**TABLE OF CONTENTS**

<b><u>ITEMS</u></b>	<b><u>PAGE</u></b>
I. Real Party in Interest	2
II. Related Appeals and Interferences	2
III. Status of Claims	2
IV. Status of Amendments	2
V. Summary of the Claimed Subject Matter	2 - 7
VI. Grounds of Rejection to be Reviewed on Appeal	7
VII. Argument	7 - 25
VIII. Conclusion	25 - 26

**APPENDICES**

I. Appealed Claims	27 - 32
II. Evidence	33
III. Related Proceedings	34
IV. Table of Cases	35
V. List of References	35